UNIVERSIDADE PAULISTA

RENAN MIRANDA RAMOS

O USO DE APLICATIVOS DE SERVIÇOS E A INSEGURANÇA MOBILE

LIMEIRA
2017

RENAN MIRANDA RAMOS

O USO DE APLICATIVOS PARA PRESTAÇÃO DE SERVIÇOS E A INSEGURANÇA MOBILE

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade de Ciências da Computação da UNIP, como requisito à obtenção do grau de Bacharel em Ciências da Computação sob a orientação do professor Mestre Sérgio Eduardo Nunes, professores Mestre Antonio Mateus Locci e Mestre Marcos Gialdi.

LIMEIRA
2017

RENAN MIRANDA RAMOS

O USO DE APLICATIVOS PARA PRESTAÇÃO DE SERVIÇOS E A INSEGURANÇA MOBILE

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade de Ciências da Computação da UNIP, como requisito à obtenção do grau de Bacharel em Ciências da Computação sob a orientação do professor Mestre Sérgio Eduardo Nunes, professores Mestre Antonio Mateus Locci e Mestre Marcos Gialdi.

Aprovada em __ de ____ de 2017.

BANCA EXAMINADORA

_____

Prof.

_____

Prof.

_____

Prof.

DEDICATÓRIA

Dedico este trabalho aos meus pais, pela perseverança, e aos professores, cujas didáticas fizeram total diferença na minha formação cidadã e acadêmica.

“A primeira regra de qualquer tecnologia utilizada nos negócios é que a automação aplicada a uma operação eficiente aumentará a eficiência. A segunda é que a automação aplicada a uma operação ineficiente aumentará a ineficiência. ” Bill Gates

LISTA DE FIGURAS

RESUMO

A análise da segurança no uso de serviços prestados no Brasil através de aplicativos mobile se faz necessária levando-se em conta o impacto desta nova forma de prestação de serviços (inéditos e já existentes). Foi possível observar através deste trabalho as contribuições que a tecnologia *mobile* tem dado para os fins mercadológicos de prestação de serviços por meio de aplicativos. Com o objetivo de salientar os principais tópicos desta relação, foi realizada uma pesquisa com usuários brasileiros de aplicativos para este fim que expôs, em primeiro momento, a necessidade da garantia da segurança das informações para acrescentar melhorias no acesso a estes serviços. Foi necessária, então, uma observância cuidadosa nos pontos que se referem à integridade, confidencialidade e disponibilidade das informações dos usuários, e constatou-se a existência de arquiteturas e protocolos que já se propõem a resolver a problemática da insegurança nesta esfera, e contatou-se, finalmente, o importante papel do fator humano na prevenção à exposição de riscos e ameaças de segurança. Foi proposto, então, um conjunto de práticas classificado como "boas práticas" de medidas preventivas através de uma cultura de segurança do ponto de vista dos usuários.

Palavras-Chave: Prestação de serviços. Aplicativos. Segurança mobile. Boas Práticas. Cultura de segurança.

ABSTRACT

The analysis of the security in the usage of services provided in Brazil through mobile applications is necessary to analyze the impact on the new structure of services (new and existing lines). It was possible to observe through this work the contributions that mobile technology has given to the marketing purposes of providing services through applications. In order to highlight the main topics of this relationship, a survey was made with Brazilian application users for this purpose, which first exposed the need of security guarantee of these information to add improvements in access to these services. A careful observance was therefore required in respect of the integrity, confidentiality and availability of users' information, and it was found that there are architectures and protocols that already propose to solve the problem of insecurity in this sphere, and finally, the important role of the human factor in preventing the exposure of security risks and threats is established. It was proposed, then, a set of practices classified as "good practices" as preventive meditations through a culture of safety from the point of view of users.

Key words: Services. Applications. Mobile Secutiry. Good pratices. Safety culture.

SUMÁRIO

1. INTRODUÇÃO

No Brasil, segundo dados da Agencia Nacional de Telecomunicações – ANATEL - o país atingiu em junho de 2017 o número de 242,1 milhões de celulares e densidade de 117,47 cel/100 hab. (ANATEL, 2017) e de acordo com a pesquisa publicada pela empresa GfK ("A importância de sempre estar acessível", 2016) 37% da população brasileira considera importante estar constantemente acessível em uma afirmação geral sobre atitudes em relação à tecnologia e necessidade constante de informação. Sendo isso colocado, principalmente no que se refere à transformação da aquisição de informação e comunicação, é bastante intuitivo imaginar que as relações de mercado foram transformadas por essa nova realidade.

Além dessas considerações, Sennes e Mendes (2009) avaliam que a internacionalização da economia brasileira expandiu os horizontes para novas estratégias - as empresas e pesquisas passaram a padrões internacionais de qualidade, trazendo investimentos externos e tornando nosso mercado mais disputado. A ideia principal dessa nova realidade é de que o mercado brasileiro se tornou não apenas seletivo, mas também mais expressivo em termos de volume de consumo. As empresas se readéquam a esses novos perfis de consumidor.

Igualmente indispensável para o crescimento econômico no mundo globalizado, a prestação de serviços auxilia as atividades de produção de bens e emprega boa parte da população (FITZSIMMONS J.; FITZSIMMONS M., 2005) além de representar quase 75% do PIB nacional brasileiro (IBGE, 2017).

Há uma readaptação na prestação de serviços através das Tecnologias da Informação Móveis e Sem Fio (TIMS). Geser (2004) aponta que essas tecnologias, como no caso dos celulares, incrementam a capacidade das empresas para administrar setores ou filiais distantes, por consequência, conseguem ser mais flexíveis - disponibilizada essa comunicação em tempo real.

Welin-Berger (2004) indica ganhos generalizados com a aplicação das TIMS nas empresas: internamente com ganhos na eficiência - por exemplo, com solicitações feitas em tempo real, redução de tarefas de campo (como relatórios de visita ao cliente) – e externamente com o acesso direto por parte dos clientes às informações do produto/serviço, tempo de entrega/agendamento, manuais técnicos/contratos de aquisição, de qualquer lugar e em tempo real.

Tem-se que considerar também a melhoria no que diz respeito à proximidade das organizações com os clientes e suas preferências (perfis), tendo como base as informações remotamente presenteadas aos prestadores de serviços (WELIN-BERGER, 2004).

A problemática da insegurança que permeava o universo dos computadores passou a assombrar a tecnologia móvel, também. A praticidade de diferentes modelos de aparatos móveis resultou na maior satisfação dos usuários, mas trouxe suas inúmeras vulnerabilidades em seus sistemas. As aplicações para cada sistema operacional cresceram com o avanço e popularização dos seus usos, e tornaram-se, por tabela, principais alvos para invasores (Batista et al., 2013).

O objetivo deste trabalho é verificar possíveis melhorias no acesso à prestação de serviços por aplicativos mobile por meio da experiência dos usuários brasileiros de aplicativos desta classe (a que nível os usuários percebem-se inseguros), uma estrutura geral dos pontos a serem compreendidos sobre segurança de aplicativos e quais melhores atitudes a serem adotadas do ponto de vista dos usuários.

2. METODOLOGIA INTRODUTÓRIA

Para que fosse possível demarcar as características dos consumidores de aplicativos prestadores de serviço, foi realizada uma pesquisa com texto em português através da ferramenta "Formulários Google" que disponibiliza com clareza a formulação de perguntas e aquisição de dados, além de auxiliar a análise das informações geradas pelas respostas.

A divulgação da enquete foi feita por meio de comunidades e sites de redes sociais e fóruns, expressamente dirigidos a participantes brasileiros no geral. Houve distribuição da enquete na Universidade Paulista de Limeira para alunos de variados cursos.

2.1 Pesquisa

A pesquisa “Serviços prestados através de aplicativos por brasileiros usuários de aplicativos para este fim" (Formulários Google) foi inicialmente nivelada por uma pergunta que confirmava o perfil de usuários dos aplicativos em questão, separando-os dos participantes que, por ventura, não utilizavam aplicativos desta categoria.

Os participantes foram questionados sobre idade, gênero biológico e renda mensal, além de serem questionados sobre a utilidade de aplicativos mobile desta categoria, se usariam um novo aplicativo para serviços de reparo/delivery através do celular ou um novo aplicativo para transporte, e se acreditam que no futuro a maioria dos serviços podem ser incrementados e disponibilizados por aplicativos mobile.

Na última parte do questionário foi apresentada uma pergunta para que definissem os aplicativos para prestação de serviços com respostas qualitativas, opcionais e múltiplas.

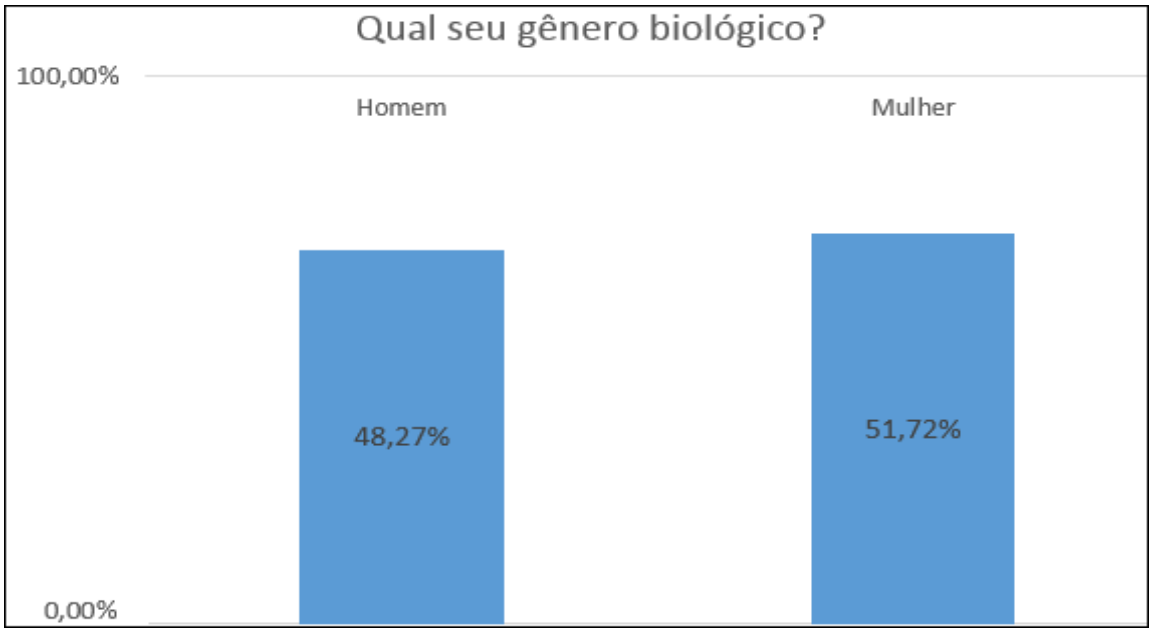
O questionário foi elaborado e disponibilizado desde o dia quinze fevereiro do ano de 2017 até o dia 01 de agosto de 2017.

2.2 Resultados

Foram contabilizados 188 participantes da enquete, sendo que quatorze participantes (7,4%) declararam não utilizar nenhum serviço por aplicativo de celular, sendo filtrados num primeiro momento e restando 174 participantes da pesquisa.

Com relação ao gênero (Figura 1), houve pouca predominância de algum dos sexos – resultando em uma amostragem bem distribuída com relação a este quesito.

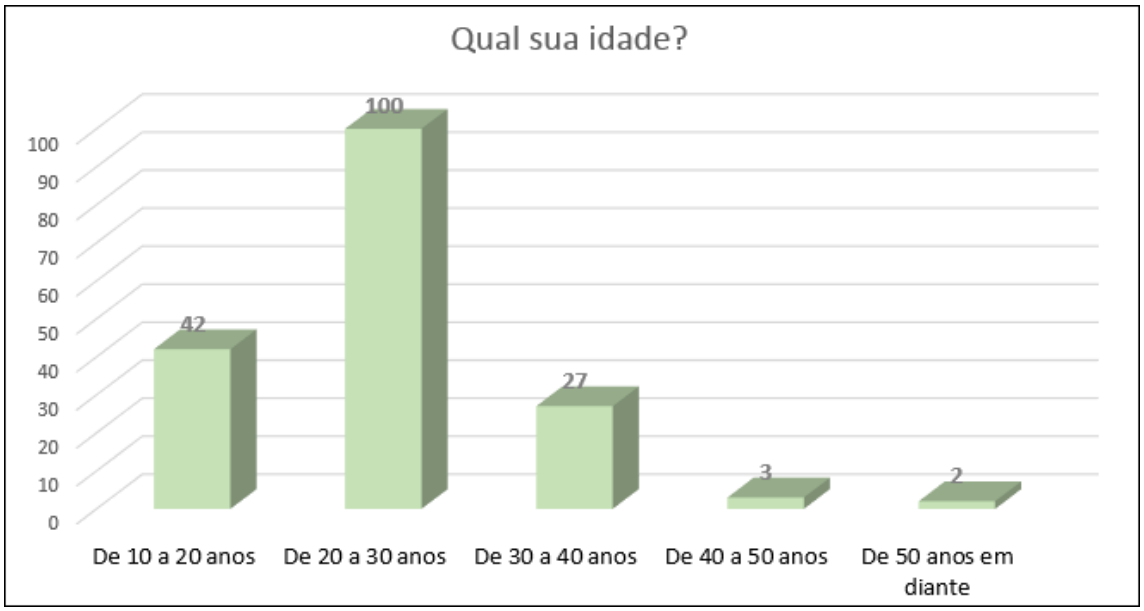
Figura 1 - Gênero dos participantes



FONTE: O Autor

Como mostra a Figura 2, a faixa etária da participação na enquete não foi muito variada, com principal participação de usuários entre 20 e 30 anos (100 participantes, 57,47%) seguidos do grupo etário de 10 a 20 anos (42 participantes, 32,7%). A faixa entre 30 e 40 anos (27 participantes) representou 15,51% da amostra, enquanto os respondentes de 40 a 50 anos de idade (3 participantes) chegaram a 1,72%. O grupo de 50 anos em diante somou 2 participantes (1,14%).

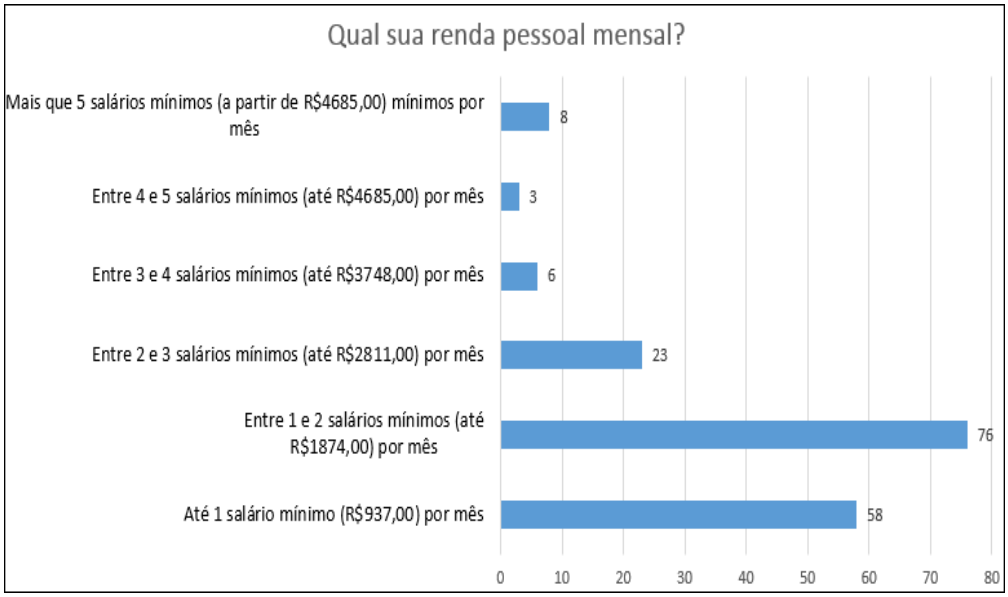
Figura 2 - Idade dos participantes



FONTE: O Autor

É possível verificar também através da Figura 3 que tanto a divulgação como a participação no questionário incluíram pessoas com diferentes rendas – e foram predominantes os participantes de renda entre até 1 e 2 salários mínimos mensais (43,7%) seguidos dos participantes cuja renda é de até 1 salário mínimo (até R$937,00) mensal (33,3%). Os respondentes de renda entre 2 e 3 salários mínimos corresponderam a 13,2%, enquanto os de renda de 4 e 5 salários mínimos representaram apenas 1,7% do total de participantes, precedidos pelos participantes de renda maior que 5 salários mínimos (4,5%).

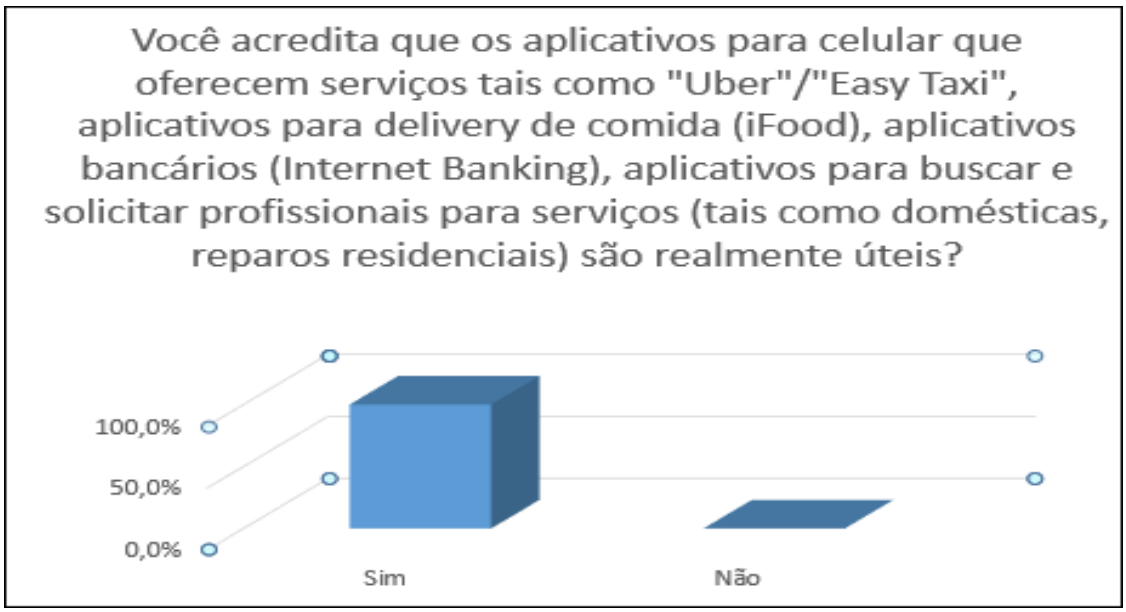
Figura 3 - Renda Pessoal Mensal



FONTE: O Autor

Quando perguntados se acreditam que os aplicativos que oferecem serviços são realmente úteis, o total da amostragem respondeu positivamente, como é possível ver na Figura 4.

Figura 4 - Utilidade de aplicativos para prestação de serviços

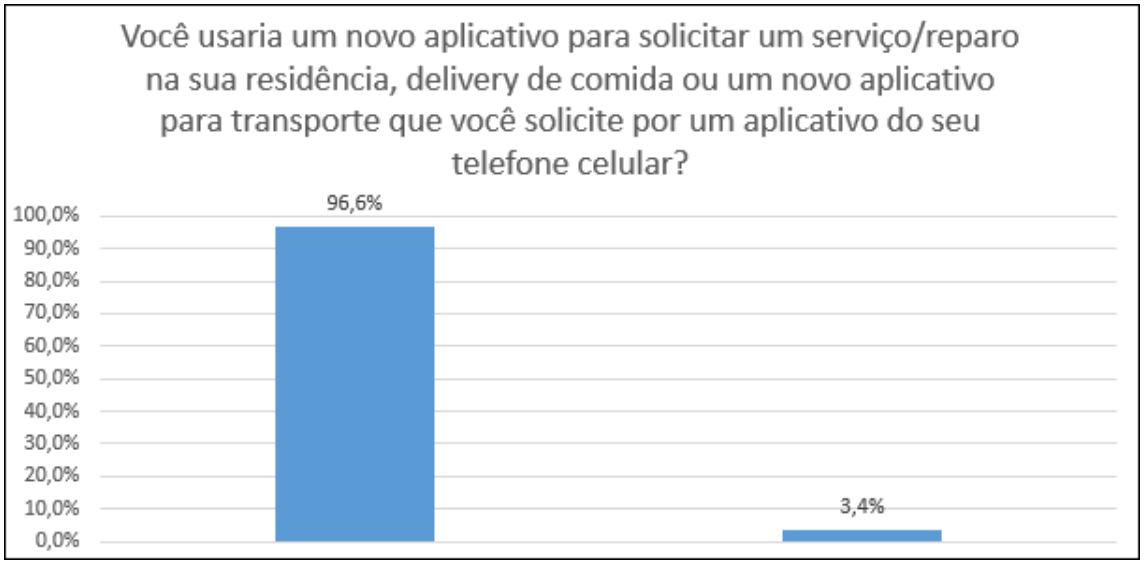


FONTE: O Autor

Ao serem questionados se usariam um novo aplicativo para solicitar um serviço/reparo na sua residência, delivery de comida ou um novo aplicativo para

transporte cujo serviço fosse solicitado por um aplicativo mobile, 96,6% da amostra respondeu positivamente, como é destacado na Figura 5.

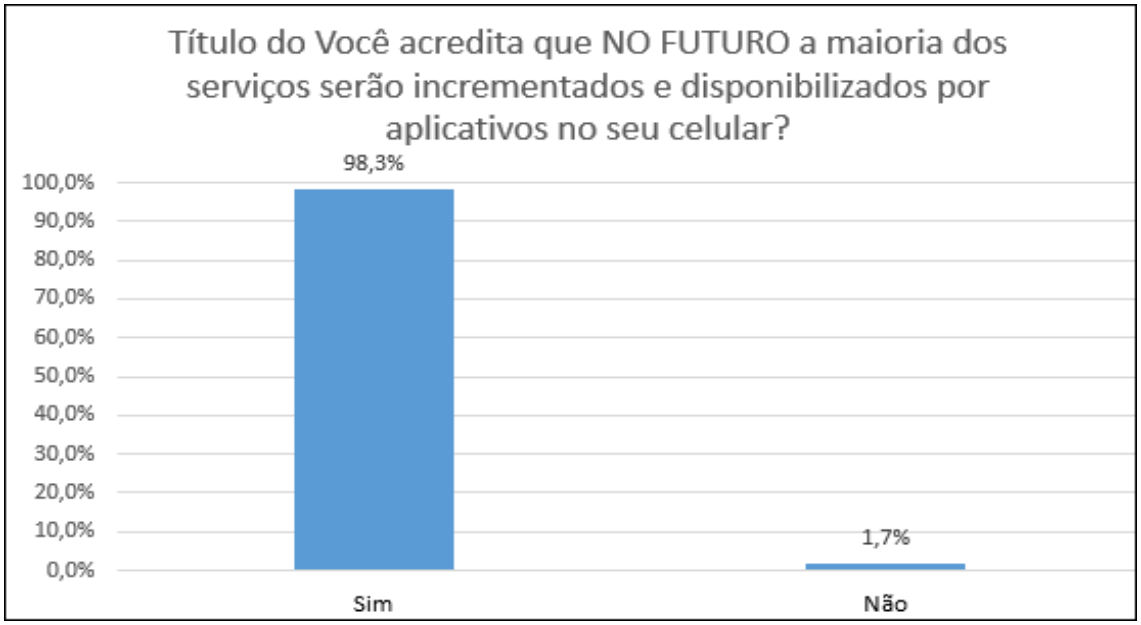
Figura 5 - Um novo aplicativo



FONTE: O Autor

Indagados sobre a crença de que no futuro a maioria dos serviços seriam incrementados e disponibilizados através de aplicativos (Figura 6) 98,3% da amostra respondeu afirmativamente.

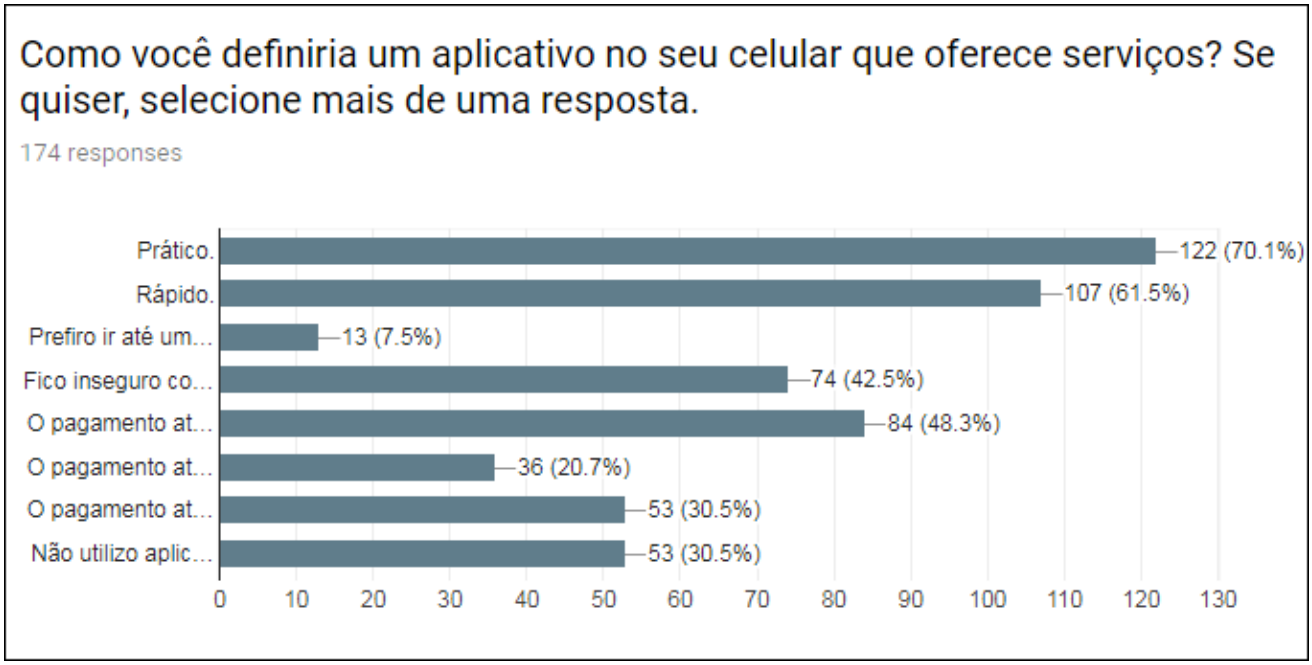
Figura 6 - Previsão de uso no futuro



FONTE: O Autor

Na Figura 7 é apresentada as classificações qualitativas dos participantes com relação à prestação de serviços por aplicativos *mobile*.

Figura 7 - Qualificações qualitativas



FONTE: O Autor

2.3 Análise da pesquisa e considerações

Apesar da clareza da receptividade positiva por parte dos usuários de aplicativos para prestação de serviços, a maior parte dos usuários estão na faixa etária dos 20 a 30 anos de idade, seguida do grupo entre 10 e 20 anos de idade - o que nos diz um pouco do perfil jovial dos usuários de aplicativos com essa finalidade. A renda mensal predominou entre usuários de 1 e 2 salários mínimos (43,7%) seguidos dos usuários de renda de até 1 salário mínimo (33,3%), ainda que haja representatividade em outras faixas renda.

Embora quase todos tenham assinalado, na questão qualitativa, as opções "Prático" (70,1%) ou "Rápido" (61,5%), 42,5% respondeu que ficam inseguros de ter as informações pessoais vazadas ("Fico inseguro de ter as minhas informações pessoais vazadas"), e 7,5% ainda prefere solicitar um serviço por uma loja física na maioria das vezes. Não houve predominância de gênero.

Mesmo que 48,3% considere o pagamento via cartão de crédito/débito bastante prático, 20,7% se diz muito inseguro com relação ao pagamento ("O

pagamento através de cartão de crédito/débito é bastante prático, mas me sinto muito inseguro"), e 30,5% se sente um pouco inseguro com relação à mesma questão das informações de pagamento (“O pagamento através de cartão de crédito/débito é bastante prático, mas me sinto um pouco inseguro"), sendo esta mesma porcentagem (30,5%) o valor de participantes que não utilizam aplicativos que envolvem pagamento.

Para que seja melhor recebida pelo mercado, a prestação de serviços por aplicativos mobile como alternativa ou único meio de se relacionar com seus clientes deve estar atenta à preocupação comum do público em relação à segurança das informações, o que aumentaria a receptividade geral dos clientes que não utilizam aplicativos que envolvem pagamento e fidelizaria na concorrência de mercado a grande fatia dos que ficam inseguros de ter as informações pessoais vazadas.

3. SEGURANÇA

Os tópicos conceituais mais estudados relacionados à Segurança de Informação são os de confidencialidade, integridade e disponibilidade (ALBUQUERQUE; RIBEIRO, 2002):

− Confidencialidade: conceito relacionado ao acesso a informações confidenciais. Em um aplicativo, apenas usuários autorizados podem ter acesso a determinadas informações.

− Integridade: está relacionada à alteração de informações. Um aplicativo cujo sistema é íntegro deve impedir que determinadas informações sejam alteradas por usuários não autorizados, e caso isto venha a ocorrer, o fato deve ser imediatamente detectado pelo sistema.

− Disponibilidade: determinadas informações de um usuário de um aplicativo, ou mesmo da empresa que o disponibiliza devem sempre estar disponíveis quando forem requisitadas.

Em se tratando de informações, elas costumam apresentar os três conceitos descritos acima, com maior ou menor ênfase, de acordo com o caso específico.

A combinação em proporções apropriadas deste tripé de segurança facilita o suporte para que as empresas alcancem os seus objetivos gerais, já que seus sistemas de informação resultam ser mais confiáveis.

Outros autores como Tipton e Krause (2005) e Sêmola (2014) defendem que para uma informação ser considera segura, o sistema que o administra ainda deve respeitar:

− Autenticação: para um usuário utilizar um determinado sistema, banco de dados ou aplicativo, ele precisa se autenticar, ou seja, dar alguma prova da sua identidade. Isso pode ser feito através do uso de uma senha, por exemplo.

− Não-Repúdio: é a garantida de que a informação chegará ao destino certo e não será ignorada ou impedida - conceito bastante importante para sistemas de transações financeiras ou de compras pela Internet. Costuma ser suportado por tecnologias de certificação digital.

− Legalidade: este conceito diz respeito à aderência de um sistema de informação à legislação em vigor.

− Privacidade: capacidade de um sistema manter sigiloso um usuário, impossibilitando a ligação direta da identidade deste com as ações praticadas por ele. É aplicado, por exemplo, no caso de eleições eletrônicas, não podendo ser possível a associação de um eleitor a um determinado voto.

− Auditoria: em sistemas de informação, o objetivo da auditoria é verificar todas as ações praticadas pelos usuários no sistema, detectando tentativas de ataque ou fraudes. É evidente que esse aspecto vai de encontro à privacidade, e por isso deve ser analisado o contexto em que se aplicam.

3.1 Vulnerabilidade mobile

Além dos riscos comuns que qualquer navegação web pode sofrer, a vulnerabilidade de dispositivos móveis alcança outro patamar: são menores, mais fáceis de perder, esquecer ou de serem furtados/roubados.

Dependem, na maioria das vezes, de conexões sem fio que vão desde conexão via infravermelho, rede móvel (2G, 3G, 4G), bluetooth e conexões WiFi - o que pode ser entendido como um conjunto de vulnerabilidades de cada tecnologia para o vazamento de informações ou como um grande alvo para ataques (SATYANARAYANAN, 2001).

Há ainda o problema da privacidade: fotos, mídias, informações pessoais que incluem localização e conversas particulares.

A preocupação com estas vulnerabilidades estende-se aos mais variados tipos de ataques, que podem surgir de várias formas. O download de aplicativos é a forma mais fácil de contaminação (PAYÃO, 2017), nas mensagens via SMS e Bluetooth também são portas de entrada latentes.

Uma das técnicas usadas por criminosos é enviar SMS com links para endereços mal-intencionados, que, ao serem clicados, instalam o malware instantaneamente. Essa mesma mensagem pode enviar dados sigilosos do usuário para o hacker que desenvolveu o malware. (VITURILLI, 2011)

Para que sejamos mais objetivos neste trabalho, trataremos das tecnologias mais utilizadas em termos de aplicativos de celular: IPSec no tráfego direto de aplicativos e o protocolo HTTPS na navegação Web.

3.2 IPSEC

O *Internet Protocol Security* – Protocolo de Segurança IP (IPSec) descrito na RFCs 2401/1998, 2402/1998 (IETF, 2017), entre outras, é uma alternativa de segurança a nível de camada de rede, criada para proteger o tráfego das informações na internet e bastante disseminada no mercado.

Pode ser utilizado diretamente nos hosts ou em dispositivos como roteadores e firewalls, e atualmente é mais utilizado nos dispositivos da infraestrutura que têm suporte ao IPSec (BRITO, 2013).

Projetado para ser usado junto ao o IPv4 para fornecer segurança para a transmissão de informações confidenciais através de redes desprotegidas, passou a ser um componente obrigatório no protocolo IPv6 (RFC 2460, 2017) junto aos seus principais elementos integrados, facilita-se sua utilização. O IPSec age na camada de rede fornecendo proteção e autenticação de pacotes IP entre dispositivos IPSec e garantindo confidencialidade, integridade e autenticidade de comunicação de dados em uma rede IP pública (Wenstrom, 2002).

É oferecido os seguintes serviços opcionais de segurança de rede:

Confidencialidade de dados - O remetente IPSec pode criptografar os pacotes antes de enviá-los através de uma rede.

A integridade dos dados - O receptor IPSec pode autenticar os pacotes enviados pelo remetente IPSec para assegurar que os dados não foram alterados durante a transmissão.

Autenticação da origem dos dados - O receptor IPSec pode autenticar a origem dos pacotes IPSec enviados. Este serviço depende do serviço de integridade de dados.

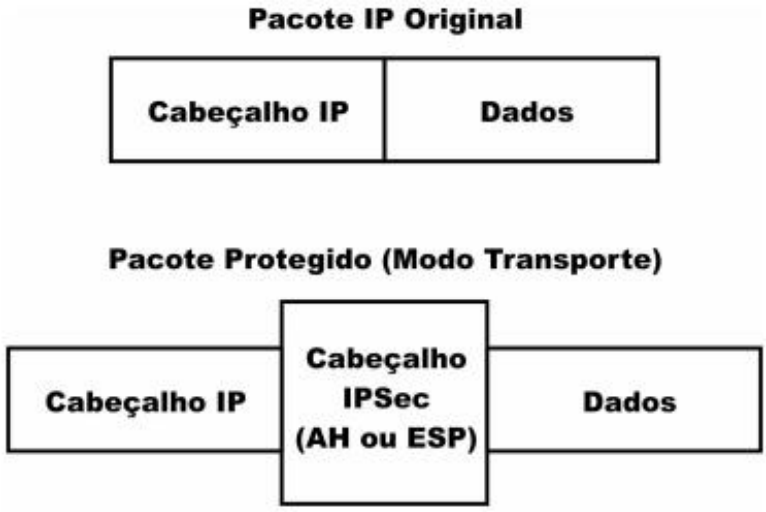
Proteção *Anti-replay* - O receptor IPSec pode detectar e rejeitar pacotes repetidos.

3.2.1 Arquiteturas de segurança

Há duas formas distintas de utilização do IPSEC: em Modo Transporte ou Modo Túnel.

Modo de transporte: aos pacotes criados neste modo são adicionados cabeçalhos IPSec entre o cabeçalho IP original e os dados em si, conforme mostrado na Figura 8.

Figura 8 - IPSEC em Modo Transporte

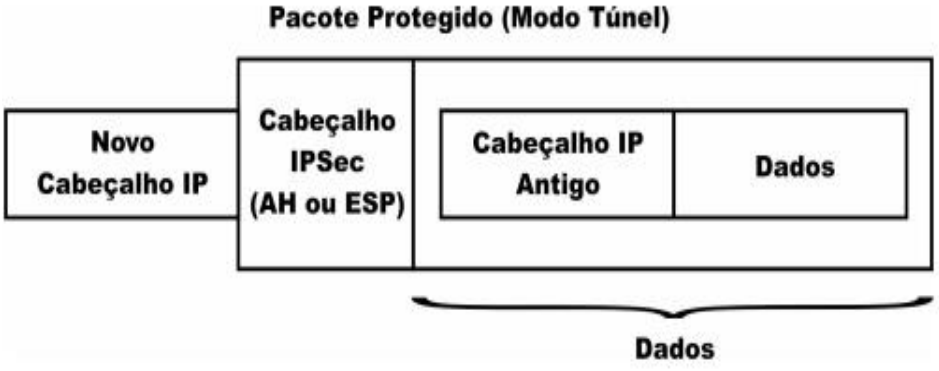


FONTE: KOLENISKOV e HATCH, 2002

Este modo é muito utilizado para computadores em diferentes redes, comunicando-se diretamente entre si, e que desejam proteger o seu tráfego IP por encapsulamento, autenticação ou ambos.

Modo de túnel: neste modo, um cabeçalho IPSec também é adicionado, à diferença de que neste modo será adicionado um novo cabeçalho IP e o pacote original será tratado como se fosse um dado só, sendo todo ele encriptado pelo cabeçalho IPSec na parte referente ao dado do novo cabeçalho, como se vê na Figura 9.

Figura 9 - IPSEC em Modo Túnel



FONTE: KOLENISKOV e HATCH, 2002

O modo túnel é comumente utilizado na comunicação entre gateways, pois fornece maior segurança aos dados originais encriptados dentro do novo pacote.

3.2.2 *Security Association* (SA)

As Associações de Segurança (SAs, em português) mantém as estruturas sigilosas para a proteção do tráfego entre computadores ou gateways, como chaves secretas ou algoritmos de criptografia. Os dados dessas associações são armazenados dentro do banco de dados “Security Association Database” (SAD), cujo acesso é restrito.

Uma associação de segurança (SA) é uma comunicação segura, protegida com IPSEC, entre duas máquinas. Para que essas duas entidades consigam enviar e receber pacotes utilizando o IPSEC é necessário o estabelecimento da SA, que escolhe os algoritmos a serem usados, as chaves de criptografia e o tempo de vida destes algoritmos, entre outros parâmetros, definindo a política de segurança e regras para envio e recebimento dos pacotes IP (TANENBAUM, 2003).

3.2.3 Frameworks de segurança do IPSEC (AH e ESP)

Os frameworks de segurança utilizam recursos independentes para realizar suas funções. O IPSEC suporta alguns algoritmos pré-definidos, que podem ser alterados de acordo com a sua maturação e necessidades. A lista de algoritmos disponíveis inclui:

- Criptografia
    - 3-DES: O Triplo DES, sigla para *Triple Data Encryption Standard* é um padrão de criptografia baseado no algoritmo de criptografia DES desenvolvido pela IBM em 1974 e tido como padrão em 1977. 3-DES usa 3 chaves de 64 bits (o tamanho máximo da chave é de 192 bits, ainda que o comprimento atual seja de 56 bits). Os dados são encriptados com a primeira chave, decriptado com a segunda chave e finalmente encriptado outra vez com a terceira chave. Isto faz o 3-DES ser mais lento que o DES original, mas oferece maior segurança. Em vez de 3 chaves, podem ser utilizadas apenas 2. (TANENBAUM, 2003).
    - *Data Encryption Standard* (DES) – É um algoritmo matemático para o processo de criptografia de informações em código binário. Usa uma chave de 64 bits mínima, da qual 56 bits definem a chave propriamente dita, e 8 bits são utilizados para fornecer detecção de erro na chave. (FARREL, 2005).
    - AES: O AES (*Advanced Encryption Standard*) é basicamente uma cifra de substituição monoalfabética que usa caracteres grandes (128 bits). Sempre que o mesmo bloco de texto simples chega ao front end, o mesmo bloco de texto cifrado sai pelo back end. Se codificar o texto simples ‘abcdefgh’ 100 vezes com a mesma chave DES, você obterá o mesmo texto cifrado 100 vezes. Um intruso pode explorar essa propriedade para ajudar a subverter a cifra. (TANENBAUM, 2003)

- Autenticação

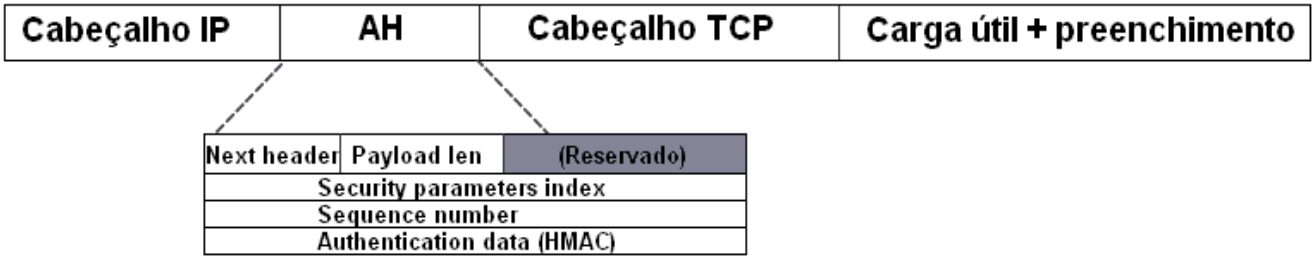
    - HMAC: *Hash-based Message Authentication Code* - Mecanismo de autenticação de mensagens utilizando funções criptográficas hash. HMAC pode ser usado com qualquer função hash, por exemplo, MD5, SHA-1, em combinação com uma chave secreta compartilhada. A força de criptografia HMAC depende das propriedades da função hash correpondente (RFC 2104, 2017)

- MD5: *Message-Digest algorithm 5* - Produz um código de autenticação de 16 bytes (a síntese de mensagem) a partir dos dados de qualquer tamanho com ou sem uma chave de qualquer tamanho. Sem uma chave, o MD5 pode ser usado para detectar mudanças acidentais nos dados. Ele pode ser aplicado mensagens individuais, estruturas de dados ou arquivos inteiros (FARREL, 2005)
- SHA1, 2 e 3: *Secure hash algorithm* - Utiliza uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits, a partir de um tamanho variável de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA se basearam no MD4 e fizeram melhorias em sua segurança. As versões 2 e 3 tiveram melhoramentos na segurança (TANENBAUM, 2003)

3.2.3.1 Cabeçalho AH

O primeiro cabeçalho é o AH (AUTHENTICATION HEADER), que possibilita a segurança e integridade para evitar reprodução, sem envolver criptografia dos dados. No IPv4 é inserido entre os cabeçalhos IP e TCP, já no protocolo IPv6 é apenas outro cabeçalho de extensão padrão deste (TANENBAUM, 2003). Sua utilização é detalhada na Figura 10.

Figura 10 - IPSEC - Authentication Header



FONTE: Adaptado de Tanenbaum 2003, p.823.

O campo deste intitulado “Next header” armazenará o que havia no campo *Protocol* do IP antes da substituição pelo número 51 que indicará a existência de um cabeçalho AH seguinte. O próximo campo “Payload lenght” será o número de palavras de 32 bits menos duas unidades que todo o cabeçalho AH conterá.

No campo “Security parameters index” será registrado o indicador da conexão – que é inserido pelo transmissor a fim de apontar um registro particular no banco de dados do receptor (o registro possui as informações da conexão e a chave compartilhada usada).

Utilizado para numeração dos pacotes enviados em uma SA, o campo “Sequence Number” distribui números exclusivos para cada pacote, ainda que em retransmissão. A finalidade deste campo é conseguir evitar ataques da ordem de reprodução. “Se todos os 2^{32} se esgotarem, terá de ser estabelecida uma nova SA para dar continuidade à comunicação” segundo Tanenbaum (2003).

O campo HMAC (Authentication data) contém a assinatura digital de carga útil negociada no estabelecimento da conexão SA entre as duas partes, já que no IPsec é utilizada uma criptografia de chave simétrica. O cálculo da assinatura é feito com a chave compartilhada (que não é transmitida).

Ainda que o cabeçalho AH não seja utilizado para criptografar os dados, é garantida a verificação da integridade, tendo o endereço do IP incluído nesse processo, não abrindo brechas para falsificação das origens dos pacotes (TANENBAUM, 2003).

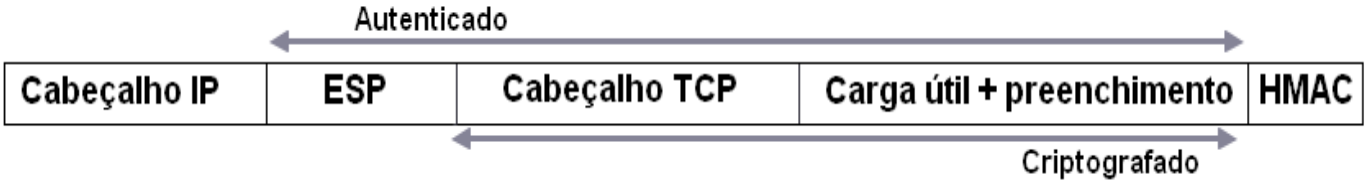
3.2.3.2 Cabeçalho ESP

O cabeçalho ESP (Encapsulating Security Payload) é um cabeçalho que garante a autenticação, confidencialidade e integridade dos pacotes, evita que os pacotes sejam reenviados, podendo criptografar os dados, garantindo que os dados trafegados pela Internet não foram alterados, além de tornar estes ilegíveis através da utilização de criptografia.

Além dos campos “Security parameters index” e “Sequenca number”, um terceiro campo é utilizado para criptografia de dados – o campo “Initialization code”.

O ESP está localizado entre o cabeçalho IP e o resto do datagrama, conforme Figura 11. Assim, os campos de dados são alterados após a criptografia dos mesmos. Cada pacote deve conter informações necessárias para estabelecer o sincronismo da criptografia, permitindo que a descriptografia ocorra na entidade de destino.

Figura 11 - IPSEC – ESP



FONTE: Adaptado de Tanenbaum 2003, p.824.

Uma situação possível de acontecer é não utilizar nenhum algoritmo de criptografia, neste caso o protocolo ESP só oferecerá o serviço de autenticação.

Já que, além da integridade, oferece sigilo e autenticação utilizando, assim como o AH, HMAC, é provável que o AH fique defasado, segundo Tanenbaum (2003).

3.3 HTTPS

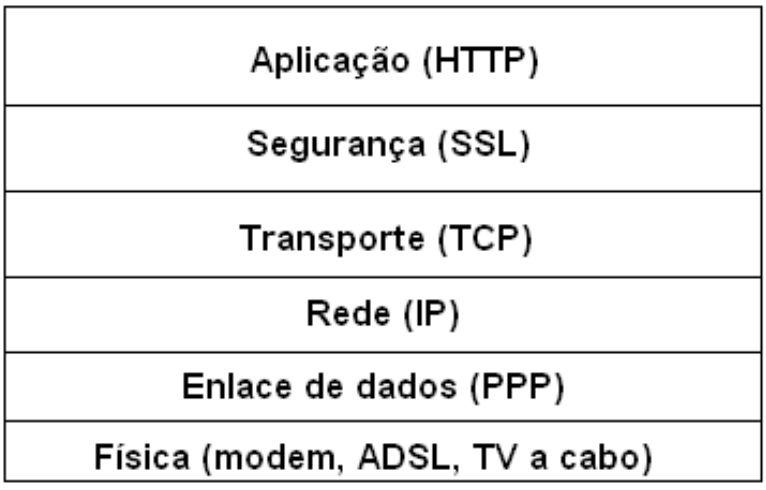
O protocolo HTTPS (HyperText Transfer Protocol Secure) é utilizado na maioria das vezes como uma opção para desenvolvimento de aplicativos quando há cobranças pelo aplicativo partindo do próprio cliente.

É acrescido o protocolo TLS/SSL (Transpor Layer Security/Secure Sockets Layer) para a implementação de segurança de um canal HTTP. Nessa abordagem, o protocolo HTTPS oferece confiabilidade contra o roubo de informações se portando como uma camada de transporte para o serviço Web, sendo muito utilizado em sites comércio eletrônico (CHOMSIRI, 2007).

3.3.1 PROTOCOLO SSL/TLS

O protocolo Secure Sockets Layer (SSL) é um protocolo originalmente desenvolvido pela Netscape para ser utilizado em seus navegadores na transmissão de dados sigilosos que oferece uma camada de segurança entre a camada de aplicação e camada de transporte, conforme a Figura 12, para duas aplicações em comunicação cuja transmissão de dados tem de ser feita de forma segura, se valendo de um protocolo de transporte confiável, tal como o TCP, para assim poder transmitir tais dados (MALCA, 2001).

Figura 12 - Camadas (e protocolos) para um usuário - SSL



FONTE: Adaptado de Tanenbaum, 2003

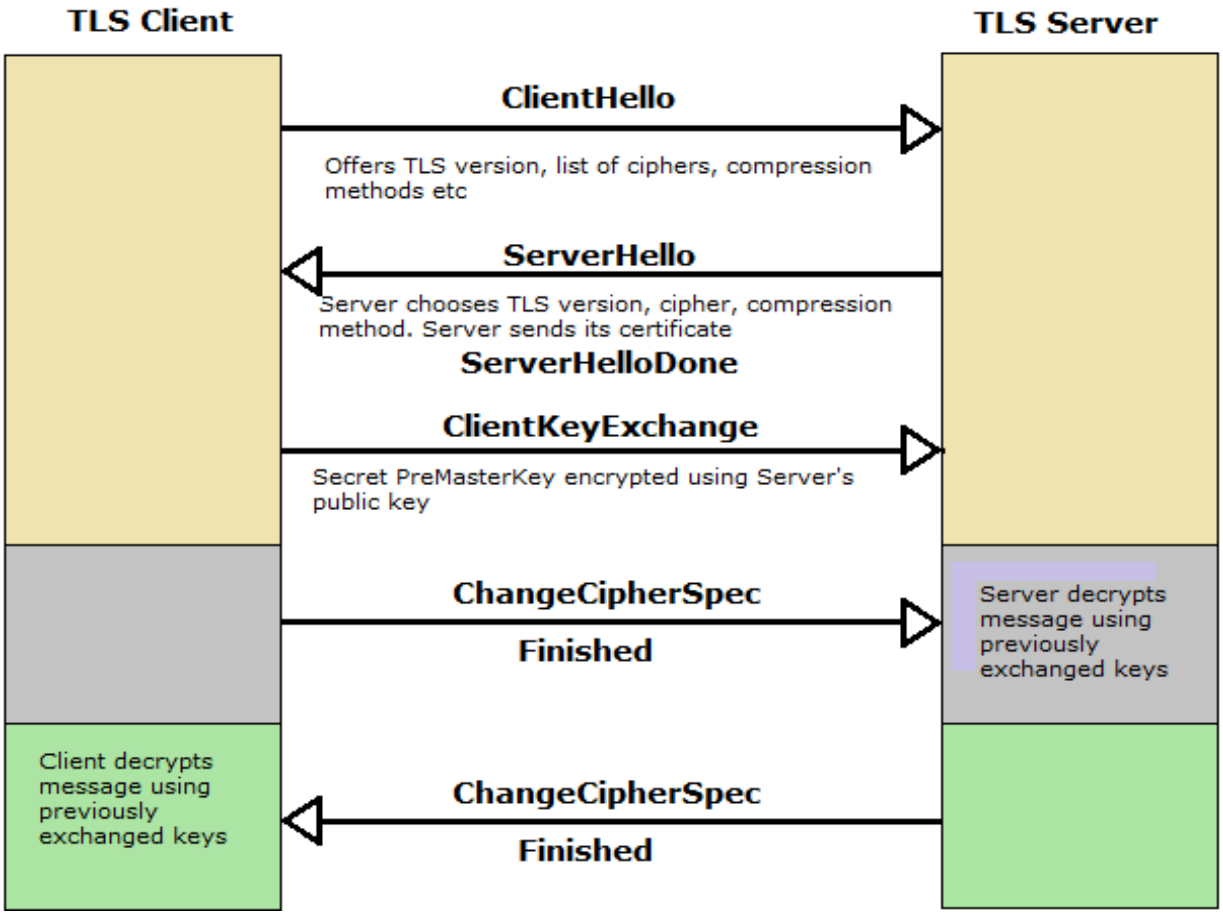
O TLS (Transpor Layer Security), sucessor do Netscape SSL, foi baseado no SSL versão 3, e é suportado pela maioria dos navegadores. Segundo Tanenbaum (2003), foram sutis as mudanças no protocolo SSL, mas o objetivo principal do protocolo TLS é prover privacidade e integridade de dados entre duas aplicações de comunicação.

Para estabelecer um canal seguro, os elementos em comunicação devem concordar com o algoritmo de encriptação a ser utilizado e quais chaves serão usadas. Para isso o TLS estabelece um handshake, para trocas de chaves simétricas utilizando criptografia de chave pública. Veremos com mais detalhes os passos dessa negociação.

- Handshake

O handshake é o início da sessão TLS, no qual o cliente e o servidor estabelecem uma conexão e trocam mensagens para definir os parâmetros criptográficos, como os algoritmos de troca de chaves, assinatura digital, confidencialidade e integridade. Nesse momento ambos também definem quais dos serviços citados acima serão utilizados na sessão em particular.

Figura 13 - TLS - Cliente/Servidor



FONTE: OPPLIGER, 2009.

A Figura 13 detalha a sequência das mensagens enviadas para o estabelecimento da sessão. Abaixo uma descrição breve de como acontece a negociação (OPPLIGER, 2009).

I - O cliente envia um “ClientHello” para o servidor, com parâmetros de configuração como a maior versão suportada, a lista de métodos de encriptação suportada e uma lista dos tipos de compressão suportadas. O servidor, então, retorna um ServerHello, com o método de encriptação escolhido e um número gerado aleatoriamente, além de seu certificado.

II - O cliente gera uma chave chamada PreMasterSecret, encriptada utilizando a chave pública do certificado do servidor. Essa chave é enviada na mensagem chamada ClientKeyExchange.

III - Finalmente o cliente e o servidor usam o número aleatório gerado no início do handshake e a PreMasterSecret para gerar a chave de sessão, finalizando a negociação.

- Integridade

O algoritmo MAC especificado pela mensagem de ServerHello garante a integridade no TLS. São utilizadas duas chaves, uma pelo servidor e outra pelo cliente, para os casos em que um está enviando e vice-versa. O elemento que envia a mensagem calcula o MAC da mensagem utilizando sua chave MAC, e a envia encriptada ao MAC. O destinatário então desencripta a mensagem e o MAC e calcula seu próprio valor do MAC. Se o resultado for igual ao MAC recebido, a mensagem está integra. Todas as versões do protocolo suportam o algoritmo de hash chamado Keyed-Hash Message Authentication (HMAC).

Utilizando o HMAC, as chaves dos MACs são derivadas da chave de encriptação compartilhada e a chave MAC do servidor e do cliente são dependentes de suas respectivas chaves MAC de escrita.

- Anti-replay

Os pacotes da sessão TLS possuem um número de sequência que é incrementado a cada envio. Caso a mensagem esteja íntegra, o número de sequência é comparado ao número sequencial anterior. Caso o número da sequência seja maior, a mensagem é processada. Esse procedimento evita ataques de replay, pois uma mensagem retida por um atacante e enviada novamente teria o número de sequência menor ou igual ao número atual.

No geral, o protocolo TSL trata de estabelecer um serviço ideal de segurança e há uma fase onde é possível se fazer variações sem se ter que projetar um novo protocolo, estas variações se referem ao uso de novos algoritmos de criptografia, tanto simétricos como assimétricos para garantir autenticidade e confiabilidade, e algoritmos para o cálculo de um código de autenticação de mensagens, que podem ser utilizados para estabelecer a camada de segurança entre duas partes.

3.4 O paradigma do fator humano

Deve ser levado em conta que a tecnologia da informação é adotada como uma representação do mundo real e virtual, gerando visões peculiares da realidade objetiva, as quais se estendem pela reflexividade de seu próprio uso – ou seja, a tecnologia aponta caminhos nunca antes enfrentados. Assim sendo, o próprio uso da tecnologia por seus usuários constitui-se em um campo aberto a diversos questionamentos e considerações, falando-se inclusive de uma “fenomenologia do ser-digital” (Kim, 2001).

Nesse sentido, Mitnick e Simon (2003) alertam que muitas organizações se preocupam em desenvolver soluções de segurança da informação com o objetivo de diminuir as vulnerabilidades relacionados ao uso dos computadores, no entanto, deixam de fora a vulnerabilidade mais significativa, que consiste no fator humano.

Hitchings (1995) apontava, já há mais de duas décadas, a necessidade de um conceito de segurança da informação no qual o aspecto do agente humano tivesse a devida relevância, fosse como agente ou paciente de eventos de segurança.

O próprio uso de senhas, como a forma mais simples de controlar o acesso de usuários a sistemas e informações, tem gerado inúmeros problemas, em função da dificuldade que a maioria das pessoas encontra para memorizar códigos. Não existe um material literário padrão que forneça procedimentos claros, passo a passo, que auxiliem na geração e na lembrança de senhas. Os usuários são obrigados a conviver com um dilema entre a segurança e a conveniência, e acabando por compartilhar suas senhas ou anotá-las em locais de fácil acesso (BROWN et al, 2004).

Sob esta perspectiva, o usuário pode ser vítima de alguém mal-intencionado, mas será parte de um comportamento social avesso aos controles tecnológicos. Ou seja, é uma ilusão imaginar que o uso de produtos de segurança padrão, da tecnologia da informação, torna as empresas imunes aos ataques.

Investir em tecnologia é muito importante para se aplicar as regras de segurança e monitorar seu cumprimento, identificar as ameaças e riscos, mas se as pessoas não forem devidamente conscientizadas no entendimento da responsabilidade de suas ações e da importância da sua participação, teremos um alto nível de insatisfação e situações de risco.

Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização (MITNICK, 2006).

Devemos conhecer os riscos e perigos a que estamos expostos para podermos agir com segurança e prevenir a existência destes incidentes ou minimizar os seus prejuízos.

3.4.1 MOTIVAÇÕES DE ATAQUES

Um ataque é caracterizado quando um hacker, utilizando um ou mais computadores, ou até mesmo uma rede, coordena a execução de várias ações direcionadas a um ou mais computadores, servidores ou redes. Essas ações têm por objetivo causar algum dano ao alvo, como esgotamento dos seus recursos, desfiguração de conteúdo ou roubo de dados confidenciais.

Para atingir seus objetivos os atacantes podem utilizar várias técnicas no ataque contra seus alvos.

De acordo com a RFC2828, “hacker é alguém com um forte interesse em computadores, que gosta de aprender sobre eles e fazer experimentos”. Muitas vezes é utilizado de maneira pejorativa, no lugar da denominação Cracker. Este sim é definido como aquele que tenta romper a segurança e ganhar acesso a sistemas que não lhe pertencem, sem ter autorização.

Os ataques que ocorrem na Internet têm como objetivo diferentes alvos através de diferentes técnicas. Qualquer aparelho móvel, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer dispositivo ou computador com acesso à Internet pode participar de um ataque.

Os motivos que levam os atacantes agir na Internet são bastante diversos, e segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) variam entre a simples diversão até a prática de crimes. Alguns exemplos são:

- Demonstração de poder: expor uma determinada organização sua vulnerabilidade à invasão e suspensão de serviços, e chantageá-la sob a ameaça de um novo ataque.

- Motivações ideológicas: publicar mensagens de cunho ideológico favorável ou contrário a uma determinada causa; bloquear ou alterar endereços web cujos conteúdos confrontem as opiniões do(s) atacante(s)

- Prestígio: competir com outros atacantes ou grupos um alvo em específico ou o maior número de ataques; destacar-se entre outros atacantes por ter logrado a invasão de sistemas, aplicativos e empresas, bloqueando seus serviços ou desfigurando seus sites tidos como difíceis alvos de ataques;

- Motivações comerciais: bloquear acesso a sites e servidores de empresas concorrentes na tentativa de denegrir a reputação da empresa e obstruir o acesso por parte da clientela.

- Motivações financeiras: adquirir informações secretas dos usuários ou empresas para realizar golpes e fraudes

3.4.2 ENGENHARIA SOCIAL

O termo ”Engenharia Social” abrange o assunto que se refere aos indicadores externos que, em geral significa o a aplicação da ciência aos

caminhos pelos quais um atacante pode lograr induzir diretamente a ação de outro indivíduo.

Para Nakamura e Geus (2003) a engenharia social é a técnica que tem como foco explorar as fraquezas sociais e humanas tendo em segundo plano a explanação da tecnologia, e que “tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização”.

Segundo um dos maiores especialistas na arte da Engenharia Social, Kevin Mitnick, a Engenharia Social “é um termo diferente para definir o uso de persuasão para influenciar as pessoas a concordar com um pedido”. (MITNICK, 2003 apud PEIXOTO, 2006)

De acordo com Peixoto (2006) a Engenharia Social retrata três aspectos fundamentais que englobam sua verdadeira essência. Uma delas é como ciência, na forma de estudo, pesquisa e descobrimento que o Engenheiro Social deve ter consigo. A técnica, como modelo de aplicação de suas habilidades envolvendo características propriamente padronizadas, personalizadas ou incrementadas. Por fim, a arte como o meio mais criativo e envolvente que o Engenheiro Social pode trazer levando em conta o senso lógico, mas, sobretudo emocional, que é muito bem explorado por esse grande articulador das vulnerabilidades humanas.

4. CULTURA DE SEGURANÇA

A “cultura de segurança” é toda uma aprendizagem que deve ser exercitada e este conhecimento pode ser repassado aos seus usuários para que os mesmos tenham comportamentos seguros e preventivos, assim como quando os transeuntes vão atravessar uma rua no semáforo verde para pedestres ou adotam sistemas de alarme para seus carros próprios. Na realidade, não estarão livres de serem atropelados simplesmente porque atravessaram a rua no sinal verde para pedestres, como também não evitarão um furto só porque trancaram o carro com o alarme.

A política de segurança da informação pode ser definida como uma série de instruções bem claras a fim de fornecer orientação para preservar as informações. Esse é um elemento essencial para o controle efetivo da segurança da informação de maneira a combater e prevenir possíveis ameaças ou ataques que venham a comprometer a segurança da informação. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social. (FONSECA, 2009).

As boas práticas para lograr a prevenção de ataques e ameaças em ambiente mobile na utilização de aplicativos seguem múltiplas ações (REVISTA ESPÍRITO LIVRE, 2017) e requerem, em grande parte, os mesmos cuidados a serem tomados com seu computador pessoal (CERTBR, 2017):

- Caso escolha utilizar um celular já usado, antes de fazer uso do aparelho restaure as configurações originais do modelo.
- Evite utilizar aparelhos cujas permissões de acesso tenham sido modificadas ou que estejam ilegalmente desbloqueados (*jailbreak*).
- Utilize um bom antivírus e *antimalware* no seu aparelho.
- Mantenha os aplicativos atualizados, bem como o sistema operacional do aparelho conforme as últimas atualizações oficiais.

- Adote senhas fortes ou biometria digital para acesso as funcionalidades do celular.

- Evite ao máximo conectar-se em redes Wi-Fi desconhecidas ou de livre acesso.

- Realize o *backup* de todas as suas informações em determinados intervalos.

- Acompanhe as notícias do fabricante, sobretudo os informativos relacionados à segurança.

- Evite instalar *plug-ins*, extensões ou aplicativos que não sejam formalmente disponibilizadas pela “Loja de aplicações” da plataforma - somente instale aplicativos que foram testados pelo fabricante do dispositivo ou do sistema operacional correspondente.

- Evite ativar interfaces de comunicação como infravermelho, *bluetooth* e Wi-Fi quando não estiver fazendo uso.

- Altere as configurações bluetooth para que não seja identificado seu aparelho facilmente ou "descoberto" por outros dispositivos.

- Configure o aparelho para possibilitar a localização e bloqueio remotos, por meio de serviços de geolocalização (pode ser muito favorável no caso de furto, roubo ou perda);

- Evite acessar *links* cuja procedência seja duvidosa ou de origem desconhecida, seja por e-mail, mensagem SMS ou outras.

- Certifique-se da posse do seu celular, sobretudo em locais de risco.

- Utilize um sistema de criptografia para informações críticas armazenadas.

- Ao se desfazer de um aparelho celular, apague todas as informações contidas no celular restaurando o modelo para as opções de fábrica.

- Em caso de furto ou perda: - altere as senhas que possam estar armazenadas de suas contas (redes sociais, e-mail, por exemplo).

- bloqueie os cartões de crédito que possam ter tido as informações armazenadas no seu dispositivo móvel.

- informe sua operadora de telefonia e requeira o bloqueio de seu número, assim como o bloqueio de seu aparelho através do número IMEI.

CONCLUSÃO

Ainda que o uso de qualquer tecnologia de informação requeira cuidados com segurança, no que tange a aplicativos de serviços para celular voltado à prestação de serviços, necessita um cuidado mais apurado uma vez que, envolvendo informações pessoais, essas informações são cada vez mais relacionadas à rotina íntima do usuário. Dados como mídias (fotos e vídeos privados, áudios de conversas), informações bancárias (aplicativos bancários, todos os aplicativos de assinatura ou que envolvam pagamento) e localização estão expostos pela navegação e uso dos aplicativos de serviços (já que estes tentam melhorar contextos mais personalizados para os usuários).

Embora todos os aparatos e algoritmos para a segurança do fluxo de informação computacional continue em evidência zelando pela integridade, confidencialidade e disponibilidade, o fator humano tem peso extra no que compete à utilização mesmo que a engenharia social tenha, em primeiro momento, foco nas organizações empresariais e a interceptação da informação desse ponto de vista – os dispositivos móveis são mais facilmente passíveis de furto, perda ou roubo e padecem da junção das vulnerabilidades das diferentes tecnologias aplicadas que podem comprometer o vazamento das informações e, conforme a resposta da amostra da pesquisa de metodologia inicial, principal insegurança e relativa resistência ao uso de aplicativos para prestação de serviços que envolvam pagamento.

Como contribuição para a insegurança dos usuários de aplicativos mobile para aplicativos de serviços, foi proposto um conjunto de tópicos de medidas de “boas práticas” para que seja promovida a prevenção da exposição das informações dos usuários.

REFERÊNCIAS

ALBERTIN, Alberto Luiz**. O comércio eletrônico evolui e consolida-se no mercado brasileiro**. RAE - Revista de Administração de Empresas. EAESP / FGV, São Paulo, Brasil, v. 40, n. 4, p.1-9, out./dez. 2000.

ALBUQUERQUE, R. e RIBEIRO, B. **Segurança no Desenvolvimento de Software**. Rio de Janeiro: Campus, 2002.

ANATEL. Agência Nacional de Telecomunicações. Disponível em: <http://www.anatel.gov.br/dados/component/content/article?id=283>. Acesso em 11 ago. 2017.

BATISTA A. L. P., Dellaquila B. L., e Balthazar G. d. R. (2013). **Análise da segurança de aplicativos na plataforma Android através da adoção de patterns**. Disponível em: <http://cbsoft2013.unb.br/wp-content/uploads/2013/09/analise-da-seguranca-de-aplicativos-na-plataforma-android-atraves-da-adocao-de-patterns.pdf>. Acesso em: 28 ago. 2017.

BRITO, S.H. B. **IPv6 - O Novo Protocolo da Internet.** São Paulo: Novatec Editora, 2013.

BROWN, A.S. et al. - Generating and remembering passwords. Applied Cognitive Psychology, 2004.

CHOMSIRI, T. HTTPS **Hacking protection. In: International Conference on Advanced Information Networking and Applications Workshops**, 2007. pg. 590-594, mai. 2007.

CERTBR. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – **Cartilha de Segurança** – Segurança em dispositivos móveis. Disponível em: <https://cartilha.cert.br/dispositivos-moveis/>. Acesso em 10 de set. 2017.

FARREL, Adrian. **A Internet e seus Protocolos:** Uma análise Comparativa. Rio de Janeiro: Elsevier, 2005

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. 16 f. Monografia (Especialização) – Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf. Acesso em: 24 ago. 2010.

GESER, H. Towards - **A sociological theory of the mobile phone**. Disponível em: <http://socio.ch/mobile/t_geser1.htm>. Acesso em 02 jul. 2017.

GFK. **A importância de estar sempre acessível** – Disponível em: <http://www.gfk.com/fileadmin/user_upload/dyna_content/BR/documents/report

s/Global-GfK-survey_Always-reachable_chart_deck_POR_v2.pdf>. Acesso em 04 de ago. 2017.

FORMULÁRIOS GOOGLE - **Serviços prestados através de aplicativos por brasileiros usuários de aplicativos para este fim**. Disponível em: <https://docs.google.com/forms/d/e/1FAIpQLScUepSX0V8StgusgjQhin1oAQb73V_Z290UIMNYWoXfscwwiw/viewform?usp=sf_link>. Acesso 13 de set. 2017.

IBGE – Agência IBGE Notícias. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/16254-pib-2-tri.html>. Acesso em 18 de set. 2017.

IETF - **The Internet Engineering Task Force** – RFC 2401/1998 – Disponível em: <https://www.ietf.org/rfc/rfc2401.txt>. Acesso em 10 de ago. 2017.

_____. RFC (Request For Comments) 2402/1998 – Disponível em: <https://www.ietf.org/rfc/rfc2402.txt>. Acesso em 14 de ago. 2017.

_____. RFC 2460/1998 – Disponível em: <https://www.ietf.org/rfc/rfc2460.txt>. Acesso em 10 de set. 2017.

_____. RFC 2828/2000 – Disponível em: <https://www.ietf.org/rfc/rfc2828.txt>. Acesso em 05 de set. 2017.

_____. RFC 2104/1997 – Disponível em: <https://www.ietf.org/rfc/rfc2104.txt>. Acesso em 10 de ago. 2017.

HITCHINGS, J. **Deficiencies of the traditional approach to information security and the requirements for a new methodology**. Computers & Security, v. 14, n. 5, p. 377–383, May 1995.

KIM, J. Phenomenology of digital-being. Human Studies, v. 24, n. 1/2, p. 87–111, Mar. 2001.

KOLENISKOV, Oleg; HATCH, Brian. **Building Linux Virtual Private Networks** (VPNs). EUA: New Riders, 2002. 385 p.

MALCA, Oscar - **Comercio electrónico**. corregida. Lima: Universidad del Pacífico, 2001

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: ataques de harckers**: controlando o fator humano na segurança da informação. São Paulo: Person Education, 2003 apud PEIXOTO, Mário César Pintaudi. Engenharia Social & Segurança da Informação na Gestão Corporativa. 1ª ed. Rio de Janeiro: Brasport, 2006.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio; **Segurança de Redes em ambientes Cooperativos**; Editora Futura; 2003.

OPPLIGER, R. **SSL and TLS:** Theory and Practice. ArtechHouse, Inc., Norwood, MA, USA, 2009

PAYÃO, Felipe **- Ataque hacker que controla smartphone pode invadir qualquer celular Android**. Disponível em:

<https://www.tecmundo.com.br/ataque-hacker/117059-ataque-hacker-controla-smartphone-invadir-qualquer-celular-android.htm>. Acesso 05 de set de 2017.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

REVISTA ESPÍRITO LIVRE. **Ameças e Vulnerabilidades em dispositivos móveis**. Disponível em: http://revista.espiritolivre.org/iiiforumrel/wp-content/uploads/2012/10/GilbertoSudre_AmeacaseVulnerabilidadesemdispositivos-moveis_IIIForumREL.pdf. Acesso em 10 de set de 2017.

SATYANARAYANAN, M. (2001). **Pervasive computing**: Vision and challenges. Personal Communications, IEEE, v. 8, n. 4, p. 10–17.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. 2. ed. Rio de Janeiro: Campus, 2014.

SENNES, R; MENDES, R. C. Políticas públicas e as multinacionais brasileiras. *In*: RAMSEY, J.; ALMEIDA, A. (Org). **A ascendência das multinacionais brasileiras:** o grande salto de peso-pesados regionais a verdadeiras multinacionais. Rio de janeiro: Elsevier, 2009.

TANENBAUM, Andrew S. **Redes de Computadores**. São Paulo: Campus, 2003.

TIPTON, H. F.; KRAUSE, M. Information Security Management Handbook. 5ª. ed. Estados Unidos: Auerbach Publications, 2005.

VITULLI, RODRIGO - **Segurança em smartphones e tablets:** saiba quais os riscos e como se proteger. Disponível em: <http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/06/27/seguranca-em-smartphones-e-tablets-saiba-quais-os-riscos-e-como-se-proteger.jhtm>. Acesso em 15 de ago. de 2017.

WELIN-BERGER, M. W. M-Commerce. In: KORNAK, A; TEUTLOFF, J; WELIN- BERGER, M. **Enterprise guide to gaining business value from mobile technologies**. Hoboken: Wiley, 2004.

WENSTROM, Michael. Managing Cisco Network Security (Gerenciando a segurança de redes CISCO). Alta Books. 2002